Популярные лекции
ПО МАТЕМАТИКЕ

Л. А. КАЛУЖНИН

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

АН
КНИГИ
НИКИТИНА

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ
ВЫПУСК 47

Л. А. КАЛУЖНИН

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ

МОСКВА 1969

511
К 17
УДК 511

СОДЕРЖАНИЕ

Введение 3
§ 1. Основная теорема арифметики. Доказательство первой части 6
§ 2. Деление с остатком и наибольший общий делитель (НОД) двух чисел. Доказательство второй части основной теоремы 9
§ 3. Алгоритм Евклида и решение линейных диофантовых уравнений с двумя неизвестными. . . 15
§ 4. Гауссовы числа и целые гауссовы числа 19
§ 5. Простые гауссовы числа и представление целых рациональных чисел в виде суммы двух квадратов 27
§ 6. Еще одна «арифметика» 30
Литература 32

Лев Аркадьевич Калужнин
Основная теорема арифметики
(Серия: «Популярные лекции по математике»)
М., 1969 г., 32 стр. с илл.

Редактор *Ф. И. Кизнер*
Технический редактор *А. А. Благовещенская* Корректор *Т. А. Понькова*

Сдано в набор 15 XI 1968 г. Подписано к печати 25/III 1969 г. Бумага 84×108¹/₃₂.
Физ. печ. л. 1. Услови. печ. л. 1,68. Уч.-изд. л. 1,54.
Тираж 150 000 экз. Т-04848. Цена 5 коп. Заказ № 1455.

Издательство «Наука»
Главная редакция физико-математической литературы
Москва В-71, Ленинский проспект, 15.

2-я типография издательства «Наука». Москва, Шубинский пер., 10

2-2-2
165-69

ВВЕДЕНИЕ

Принято считать, что арифметика предшествует алгебре, что это более элементарная часть математики. В школе арифметике учат начиная с первого класса, а алгебре — только с пятого. Так как подавляющее большинство людей знает о математике главным образом то, что они услышали в школе, то мнение об элементарности арифметики глубоко укоренилось. Между тем арифметика, если ее понимать как учение о свойствах целых чисел и о действиях над ними,— трудный и далеко не элементарный раздел математики. Правда, в таком общем понимании этот раздел принято скорее называть «высшая арифметика» или «теория чисел», чтобы противопоставить его школьной арифметике. Но эти названия не должны затемнять суть дела. А она состоит в том, что и школьная арифметика и высшая арифметика относятся к одной и той же области знания. На мой взгляд, было бы очень полезно, если бы школьники старших классов, имеющие склонность к математике, углубляли тот набор знаний, который они приобрели в младших классах. Такое углубление необходимо, впрочем, и для того, чтобы в дальнейшем познакомиться с высшей арифметикой. Цель нашей брошюры — помочь в этом деле.

В качестве отправного пункта мы рассмотрим так называемую основную теорему арифметики. Это несколько наукообразное название не должно отпугивать: все эту теорему хорошо знают и при арифметических вычислениях часто ею пользуются (например, при нахождении общего знаменателя дробей), не сознавая порой того, что это — глубокая теорема, требующая внимательного и подробного доказательства. Поясним, о чем идет речь:

Каждое целое число мы умеем раскладывать в произведение простых чисел. Например,

$$420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7. \qquad (1)$$

При этом, если число достаточно велико, для нахождения соответствующего разложения нужно иногда потратить немало времени. Тем не менее, во всех случаях мы это разложение при желании всегда устанавливаем. Но, может быть, нам до сих пор просто везло? Уверены ли мы в том, что произвольное целое число можно всегда представить в виде произведения простых чисел? Это действительно так, но этот факт требует доказательства. Первую часть основной теоремы как раз и составляет утверждение:

Всякое целое число может быть представлено в виде произведения простых чисел.

Доказательство этого утверждения приводится в брошюре. Впрочем, оно довольно простое и читателю было бы полезно провести его самостоятельно. Труднее доказывается второе утверждение теоремы (которое, однако, в школе считают очевидным). Прежде чем переходить к его формулировке, обратимся опять к рассмотренному выше примеру разложения числа 420 на простые сомножители. Процедура, хорошо известная со школы и схематически изображающаяся так:

420	2
210	2
105	3
35	5
7	7
1	

,

как раз и дает разложение (1). Но может быть существуют и другие методы разложения? Как знать, дадут ли они тот же результат. Естественно, например, пытаться разложить данное число в произведение двух меньших чисел (не обязательно взаимно простых), а затем каждое из них — в произведение меньших чисел и т. д., до тех пор, пока мы не придем к числам, уже не разложимым далее (т. е. к простым). Однако уже из первого шага ясно, что такой процесс неоднозначен. Действительно, например, для того же числа

420 имеем:

$$420 = 20 \cdot 21, \qquad 420 = 15 \cdot 28.$$

Таким образом, совершенно естествен вопрос: быть может существуют целые числа, которые можно разложить различными способами в произведение простых чисел? Оказывается, что таких целых чисел нет, и соответствующее утверждение — утверждение об однозначности разложения числа в произведение простых сомножителей — составляет как раз вторую часть основной теоремы:

Если некоторое целое число n разложено двумя способами в произведение простых сомножителей

$$n = p_1 p_2 \ldots p_k = q_1 \cdot q_2 \ldots q_l,$$

то эти разложения совпадают с точностью до порядка сомножителей: оба они обладают одним и тем же числом сомножителей, $k = l$, и каждый сомножитель, встречающийся в первом разложении, встречается столько же раз во втором разложении [1]).

Доказательство этого утверждения мы приведем довольно подробно. Оно, как уже отмечалось, существенно труднее, чем доказательство первого утверждения. Эта трудность не случайна, а связана с глубокими свойствами арифметики целых чисел. Оказывается, что наряду с этой привычной арифметикой существуют, и очень полезны, многочисленные другие «арифметики». В одних арифметиках утверждения основной теоремы справедливы, в других — нет, причем не выполняется как раз утверждение об однозначности разложения. Мы приведем примеры арифметик как первого, так и второго рода.

Более подробно мы рассмотрим одну арифметику первого рода — арифметику целых комплексных чисел, или, как их обыкновенно называют, целых гауссовых чисел. Отметим, кстати, что обычные целые числа (чтобы не спутать их с целыми гауссовыми числами) мы будем иногда называть целыми рациональными числами. Однако там, где это не может вызвать недоразумений, мы будем

---

[1]) Если рассматривать произвольные целые числа (как положительные, так и отрицательные), то под единственностью разложения на простые множители следует понимать, что два разложения $n = p_1 \cdot p_2 \ldots \ldots p_k$ и $n = q_1 \cdot q_2 \ldots q_l$ могут отличаться не только порядком сомножителей, но и знаками соответствующих сомножителей; см. § 1—формулировку основной теоремы.

говорить просто о целых числах, имея в виду целые рациональные числа. В арифметике целых гауссовых чисел основная теорема также выполняется и ее выполнимость влечет за собой целый ряд интересных и далеко не очевидных свойств целых рациональных чисел

В конце брошюры мы приведем пример арифметики, в которой основная теорема не выполняется: правда, рассматриваемые там числа можно разложить в произведение простых сомножителей, но при этом может оказаться, что простые числа, встречающиеся в двух разложениях, различны. Более детально мы не будем исследовать эту арифметику: это потребовало бы введения ряда новых понятий и изучения их свойств, что возможно только в рамках серьезного университетского курса.

Для понимания нашего изложения читателю не потребуется познаний, отличных от тех, которые излагаются в школьном курсе математики, за одним важным исключением. При доказательстве теорем мы будем широко пользоваться методом математической индукции [1]). Этот центральный для математики метод, к сожалению, редко рассматривается в школе. Подробное обоснование и пояснение этого метода завело бы нас слишком далеко от нашей темы. Читателю, который хочет познакомиться с методом доказательства по индукции, мы можем порекомендовать брошюру И. С. Соминского «Метод математической индукции», вышедшую в серии «Популярные лекции по математике», либо книгу И. С. Соминского, Л. И. Головиной и И. М. Яглома «О математической индукции» («Наука», 1967).

В конце брошюры мы укажем некоторые книги, излагающие в доступной форме теоретико-числовые факты, более или менее тесно примыкающие к изучаемому здесь вопросу.

§ 1. ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ. ДОКАЗАТЕЛЬСТВО ПЕРВОЙ ЧАСТИ

Дадим единую формулировку для высказанных во введении утверждений, т. е. сформулируем полностью основную теорему арифметики.

Всякое целое число, отличное от нуля, может быть представлено в виде произведения простых чисел, причем такое

---

[1]) Иногда ее называют также «полной индукцией».

представление единственно с точностью до порядка сомножителей и их знаков.

Как уже говорилось, указанная теорема содержит два утверждения: во-первых, утверждение о существовании представления произвольного числа в виде произведения простых чисел, и во-вторых, утверждение о единственности такого представления. Оба утверждения будут нами доказаны: в настоящем параграфе — только первое из них. Предварительно сделаем два простых замечания.

1. Число 1 по многим причинам не принято считать простым числом, несмотря на то, что оно не разложимо в произведение меньших чисел. Тогда возникает вопрос: в каком же смысле указанная выше теорема верна для числа 1? Или, иначе, в каком смысле 1 представима в виде произведения простых чисел? Математика, в отличие, скажем, от грамматики, не любит исключений. Мы будем считать, что

$$1 = 1$$

и есть разложение числа 1 в произведение простых чисел, причем число простых сомножителей в правой части равно 0. Эта условность напоминает определение нулевой степени $a^0 = 1$ (число сомножителей a равно 0) и во многих отношениях удобно. Подобное соглашение мы принимаем и для числа -1.

2. В качестве второго замечания мы просто приведем пример, поясняющий понятие однозначности разложения целого числа на простые сомножители. Два разложения числа 18

$$18 = 2 \cdot 3 \cdot 3$$

и

$$18 = (-3) \cdot (-2) \cdot 3$$

мы считаем неразличимыми.

Доказательство существования разложения целого рационального числа в произведение простых чисел. Ограничимся сначала случаем положительных целых чисел. Возможность их разложения на простые сомножители доказывается методом математической индукции:

а) Для $n = 1$ $1 = 1$ и есть искомое представление: 1 является произведением пустого множества простых чисел.

б) Предположим, что для всех положительных чисел m, меньших чем n, разложимость в произведение простых чисел уже установлена. Докажем тогда, что и для числа n такая разложимость будет иметь место. Если n — п р о с т о е число, то

$$n = n$$

и есть искомое разложение (один простой сомножитель). Пусть n — число с л о ж н о е. Тогда оно является произведением $n = n_1 \cdot n_2$ двух целых чисел n_1 и n_2, каждое из которых отлично от 1 и n и, следовательно, $n_1 < n$ и $n_2 < n$. Но тогда, по предположению индукции, разложимость чисел n_1 и n_2 в произведение простых чисел уже установлена:

$$n_1 = p_1 \cdot p_2 \ldots p_r,$$

$$n_2 = q_1 \cdot q_2 \ldots q_s,$$

где p_j и q_l — простые числа. Имеем $n = p_1 \cdot p_2 \ldots p_r \cdot q_1 \cdot q_2 \ldots$ $\ldots q_s$, т. е. мы получили искомое разложение числа n.

Если же n — отрицательное целое число, то $-n$ — число положительное. Как уже доказано, $-n$ разложимо в произведение простых чисел. Пусть

$$-n = p_1 \cdot p_2 \ldots p_k,$$

тогда

$$n = (-1) p_1 \cdot p_2 \ldots p_k,$$

или, например,

$$n = (-p_1) \cdot p_2 \ldots p_k$$

— искомое разложение числа n. Тем самым первая часть теоремы доказана.

Доказательств единственности разложения существует довольно много. То, которое мы приведем, не самое короткое и не самое простое. Однако наше доказательство имеет то преимущество, что оно непосредственно обобщается на ряд других областей, например, на область полиномов от одной переменной и на область целых комплексных чисел. Кроме того, по ходу доказательства, в некотором смысле в виде побочной продукции, мы получим ряд других важных теорем арифметики.

§ 2. ДЕЛЕНИЕ С ОСТАТКОМ И НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ (НОД) ДВУХ ЧИСЕЛ. ДОКАЗАТЕЛЬСТВО ВТОРОЙ ЧАСТИ ОСНОВНОЙ ТЕОРЕМЫ

Исходным для наших рассмотрений является утверждение о возможности «деления с остатком» в области целых чисел. Точно это утверждение формулируется так:

Теорема 1. *Пусть a и b — целые числа и $b \neq 0$. Тогда существуют такие целые числа q и r* [1], *причем* $0 \leqslant |r| < b$, что

$$a = q \cdot b + r. \tag{1}$$

Равенство $r = 0$ в представлении (1) равносильно тому, что число a делится на b [2]). Этот факт мы в дальнейшем будем записывать так: $b \mid a$ — такая запись принята в теории чисел.

Докажем возможность такого представления. Заметим для этого, что для каждого рационального числа τ найдется такое целое число t, что $|\tau - t| < 1$ [3]). Пусть $\tau = \frac{a}{b}$; a и b — целые числа. Подберем такое целое число q, чтобы $\left|\frac{a}{b} - q\right| < 1$, и положим

$$r = b\left(\frac{a}{b} - q\right) = a - bq.$$

Итак, r — целое число, $|r| = |b|\left|\frac{a}{b} - q\right| < |b| \cdot 1 = |b|$ и

$$a = q \cdot b + r,$$

что и требовалось доказать [4]).

---

[1]) Остаток r может быть произвольным целым числом — положительным, отрицательным или нулем.

[2]) Для двух целых чисел a и b выражения «число a делится на число b», «число a — кратное числа b», «число b является делителем числа a» или, наконец, «число b делит число a» имеют один и тот же смысл; мы будем пользоваться каждым из них.

[3]) В действительности ближайшее к числу τ целое число отличается от него не больше, чем на $\frac{1}{2}$, но нам это уточнение не понадобится.

[4]) Отметим, что в представлении (1) целые числа q и r определены не однозначно. Например, для $a = 13$ и $b = 3$ имеем $13 = 4 \cdot 3 + 1$ ($q = 4$, $r = 1$) или $13 = 5 \cdot 3 + (-2)$ ($q = 5$, $r = -2$). Это видно также

Теорема 1 позволяет ввести понятие наибольшего общего делителя двух чисел и доказать ряд его свойств.

Определение 1. Если a и b — два целых числа, отличных от нуля, и если число c таково, что $c \mid a$ и $c \mid b$, то c называется *общим делителем* чисел a и b. Заметим, что произвольные два числа всегда обладают общими делителями; таковыми являются числа 1 и —1. Если других общих делителей нет, то числа a и b называются *взаимно простыми*. О взаимно простых числах мы поговорим ниже.

Определение 2. Число d называется *наибольшим общим делителем* чисел a и b (НОД), если: 1) d является общим делителем чисел a и b и 2) d делится на любой другой общий делитель чисел a и b. (Так, например, 6 есть НОД чисел 18 и 30, так как $6 \mid 18$ и $6 \mid 30$ и, с другой стороны, 6 делится на все общие делители этих чисел: 1, —1, 2, —2, 3, —3, 6, —6).

Читателю еще со школы известно, что для любой пары целых чисел существует НОД, причем известен также метод его нахождения. Но если припомнить и внимательно проанализировать этот метод, то можно без труда заметить, что он использует разложение чисел a и b на простые множители и однозначность такого разложения. Этот путь для нас сейчас закрыт, так как мы как раз только собираемся доказать соответствующую теорему.

Из нашего определения (определение 2) непосредственно не видно, что для произвольных двух чисел a и b НОД всегда существует. Мы сейчас докажем, что это действительно так, причем доказательство не будет использовать разложение чисел a и b на простые сомножители.

Теорема 2. *Для любой пары целых чисел* $a \neq 0$ *и* $b \neq 0$ *существует* НОД.

Доказательство. Наряду с числами a и b мы будем рассматривать всевозможные числа вида $xa + yb$, где x и y — какие-либо целые числа. Числа такого вида

$$v = xa + yb \qquad (2)$$

мы будем называть *линейными комбинациями* чисел a и b.

из нашего доказательства. Действительно, если a не делится на b, то $\frac{a}{b}$ — дробное число, но тогда $n < \frac{a}{b} < n + 1$, где n — некоторое целое число. В качестве числа q можно выбрать $q = n$ или $q = n + 1$, что и дает два представления вида (1). Только в случае, когда $b \mid a$, число q однозначно определено: $a = q \cdot b$; при этом остаток $r = 0$.

Например, для $a = 6$, $b = 22$ линейными комбинациями будут числа 28 ($28 = 1 \cdot 6 + 1 \cdot 22$), 10 ($10 = (-2) \cdot 6 + 1 \cdot 22$), -92 ($-92 = 3 \cdot 6 + (-5) \cdot 22$) и т. д. Вообще для заданных чисел a и b существует бесконечно много чисел, являющихся их линейными комбинациями. Обозначим множество таких чисел через M. Заметим, что множество M содержит, в частности, и сами числа a (для $y = 0$, $x = 1$) и b (для $x = 0$, $y = 1$), а также число 0 ($x = 0$, $y = 0$). Все числа v из множества M являются, очевидно, целыми числами. Если v принадлежит M, то и $-v$ тоже принадлежит M (если $v = xa + yb$, то $-v = (-x)\ a + (-y)b$). Отметим еще одно свойство чисел v из M, которое нам сразу понадобится: все такие числа делятся на все общие делители чисел a и b. Действительно, если $c \mid a$ и $c \mid b$, и, скажем, $a = a'c$ и $b = b'c$, то $v = xa + yb = xa'c + yb'c = (xa' + yb')\ c$, т. е. $c \mid v$. Пусть теперь $d \neq 0$ — наименьшее по модулю число среди всех чисел из M, отличных от 0 [1]). Мы покажем, что d и является НОД чисел a и b. Свойством 2) определения НОД оно обладает, так как им обладают все числа из M. Нужно только еще установить, что оно обладает и свойством 1), т. е. что d является общим делителем чисел a и b. Покажем, что $d \mid a$. Так как d принадлежит M, то оно представимо в виде $d = sa + tb$, где s и t — подходящие целые числа. Разделим a на d с остатком, т. е. найдем такие числа q и r, $|r| < |d|$, что

$$a = qd + r.$$

Но тогда и остаток r должен принадлежать множеству M. Действительно,

$$r = a - qd = a - q\ (sa + tb) = (1 - qs)\ a + tb.$$

Вспомним теперь, что d – наименьшее по модулю число среди отличных от нуля чисел множества M, а число r меньше d. Следовательно, $r = 0$ и $d \mid a$. Дословно также доказывается делимость $d \mid b$. Теорема доказана.

Мы установили существование НОД двух целых чисел, отличных от нуля. Более того, из доказательства мы

[1]) Такое число в множестве M действительно существует. Заметим, что в множестве M содержатся числа, не равные нулю (например, a или b), а их модули — положительные целые, т. е. натуральные, числа. Но одно из основных свойств натуральных чисел, принимаемое обычно за аксиому (см. И. С. Соминский, «Метод математической индукции», стр. 9, замечание), состоит в том, что во всякой непустой совокупности натуральных чисел всегда содержится наименьшее число.

усматриваем следующий важный факт, который нам вскоре понадобится:

Теорема 3. НОД *чисел a и b представим в виде линейной комбинации этих чисел.*

Возникает вопрос: определен ли НОД чисел a и b однозначно? Ответ, конечно, отрицательный: если число d обладает свойствами 1) и 2) определения НОД, то и $-d$ тоже ими обладает. Но этим неоднозначность исчерпывается. Действительно, пусть d и d' — два НОД чисел a и b. Так как d обладает свойством 2), а d' — свойством 1), то $d' \mid d$. Но аналогично, $d \mid d'$. Итак, $\alpha = \frac{d}{d'}$ и $\frac{d'}{d} = \frac{1}{d/d'} = \frac{1}{\alpha}$ — целые числа. Но единственные целые числа, обратные от которых также целые,— это числа 1 и -1. Итак, $\alpha = 1$ или $\alpha = -1$, откуда $d' = d$ или $d' = -d$. Если бы мы в определении НОД потребовали, чтобы это число было положительным — это иногда (но далеко не всегда) бывает удобным,— то можно было бы сказать, что НОД *двух отличных от нуля целых чисел существует и однозначно определен.*

В дальнейшем мы будем обозначать НОД чисел a и b через (a, b), как это обычно принято в литературе по теории чисел.

Перейдем к рассмотрению пар взаимно простых чисел. Мы уже встречались с этим понятием. Повторим его определение.

Определение 3. Целые числа $a \neq 0$ и $b \neq 0$ называются *взаимно простыми*, если их НОД равен 1.

Иными словами, можно сказать, что взаимно простые числа — это такие числа, единственными общими делителями которых являются числа 1 и -1.

Из сказанного выше (теорема 3) следует, что если $(a, b) = 1$, то 1 представима в виде

$$1 = sa + tb \tag{3}$$

с подходящими целыми числами s и t. Обратно, если равенство (3) выполняется для подходящих s и t, то a и b взаимно просты. Действительно (см. доказательство теоремы 1), $d = (a, b)$ — это наименьшее по модулю число среди отличных от нуля чисел вида $xa + yb$. Следовательно, если (3) выполняется, то $|d| \leqslant 1$ и $d \neq 0$, так что $d = \pm 1$.

Из сказанного сразу следует важнейшее свойство взаимно простых чисел.

Теорема 4. *Если* $a|bc$ *и* $(a, b) = 1$, *то* $a|c$ (это свойство читается так: *если число* a *делит произведение двух чисел и взаимно просто с одним из сомножителей, то оно делит другой сомножитель*).

Доказательство. Так как $(a, b) = 1$, то найдутся такие числа s и t, что

$$1 = sa + tb. \tag{4}$$

Умножим последнее равенство на c. Имеем

$$c = (sc)a + t(bc).$$

Оба слагаемых в правой части делятся на a, следовательно, c делится на a.

Полезно также следующее утверждение.

Теорема 5. *Если число* a *взаимно просто с числами* b *и* c, *то оно взаимно просто с произведением* bc.

Доказательство. Так как $(a, b) = 1$, то найдутся целые числа s и t, удовлетворяющие равенству

$$1 = sa + tb.$$

Аналогично, так как $(a, c) = 1$, то

$$1 = ua + vc$$

для подходящих u и v. Перемножив почленно два последних равенства, получаем

$$\begin{aligned} 1 &= (sa + tb)(ua + vc) = \\ &= sua^2 + savc + tbua + tbvc = \\ &= (sua + svc + tbu)a + (tv)\cdot(bc). \end{aligned}$$

Положим $m = sua + svc + tbu$ и $n = tv$, тогда m и n — целые числа и

$$1 = ma + n(bc),$$

и это показывает, что a и bc взаимно просты.

Утверждение последней теоремы легко обобщается на произвольное число сомножителей:

Теорема 6. *Если* a *взаимно просто с числами* $b_1, b_2, \ldots, b_k$, *то* a *взаимно просто с произведением* $b_1 \cdot b_2 \ldots b_k$.

Доказательство этой теоремы проводится методом математической индукции по числу k сомножителей.

Доказательство единственности разложения целого числа в произведение простых сомножителей.

Теперь, наконец, мы можем доказать вторую часть основной теоремы арифметики. Для этого заметим, что по самому определению простого числа два различных простых числа взаимно просты. Доказательство однозначности разложения будем вести индукцией по абсолютной величине числа n.

а) Если $|n| = 1$, то $n = \pm 1$ и

$$1 = 1, \qquad -1 = -1,$$

т. е. имеет место единственность разложения для чисел 1 и -1.

б) Предположим, что доказываемое свойство уже установлено для всех чисел m, для которых $|m| < |n|$. Пусть

$$n = p_1 \cdot p_2 \ldots p_k = q_1 \cdot q_2 \ldots q_l$$

— два разложения числа n в произведение простых чисел $p_1, p_2, \ldots, p_k$ и $q_1, q_2, \ldots, q_l$ соответственно. Мы утверждаем, что простое число p_k встречается среди простых чисел $q_1, q_2, \ldots, q_l$ (или, быть может, противоположно какому-то из них). Действительно, если бы это было не так, т. е. $p_k \neq \pm q_i$, $i = 1, 2, \ldots, l$, то p_k было бы взаимно просто со всеми числами q_i, а следовательно, согласно теореме 6 оно было бы взаимно просто с их произведением, т. е. с числом n. Но это невозможно, так как $p_k \mid n$, т. е. $(p_k, n) = p_k$. Итак, p_k равно какому-то из простых чисел $\pm q_i$. Можно считать, что $p_k = q_l$, так как в противном случае такого равенства можно было бы добиться перестановкой сомножителей q_i, а затем, если все же $p_k = -q_l$, изменением знака у q_l с изменением его у какого-либо другого q_i.

Итак, получаем:

$$n = p_1 \cdot p_2 \ldots p_{k-1} \cdot p_k = q_1 \cdot q_2 \ldots q_{l-1} \cdot p_k,$$

откуда

$$m = \frac{n}{p_k} = p_1 \cdot p_2 \ldots p_{k-1} = q_1 \cdot q_2 \ldots q_{l-1}.$$

Но $|m| < |n|$ и, по предположению индукции, для m утверждение теоремы уже доказано, т. е. $k - 1 = l - 1$, последовательности $p_1, p_2, \ldots, p_{k-1}$ и $q_1, q_2, \ldots, q_{l-1}$ содержат с точностью до знаков одни и те же простые числа, и соответствующие простые числа встречаются в обоих представлениях одно и то же число раз, а так как $p_k = q_l$, то это же верно и для последовательностей $p_1, p_2, \ldots, p_{k-1}, p_k$ и $q_1, q_2, \ldots, q_{l-1}, q_l$. Теорема доказана.

§ 3. АЛГОРИТМ ЕВКЛИДА И РЕШЕНИЕ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ С ДВУМЯ НЕИЗВЕСТНЫМИ

Согласно теореме 2 два целых числа a и b обладают НОД. Опишем сейчас одну процедуру нахождения НОД, которая была указана еще в «Элементах» Евклида и называется *алгоритмом Евклида*.

При этом будем считать, что $|a| \geqslant |b|$.

Первый шаг. Делим a на b с остатком:

$$a = q_1 \cdot b + r_1, \qquad |r_1| < |b|. \tag{1}$$

Если $r_1 = 0$, то $b|a$ и $(a, b) = b$. Если $r_1 \neq 0$, то делаем

Второй шаг. Делим b на r_1:

$$b = q_2 \cdot r_1 + r_2, \qquad |r_2| < |r_1|. \tag{2}$$

Если $r_2 \neq 0$, то делаем

Третий шаг.

$$r_1 = q_3 \cdot r_2 + r_3, \qquad |r_3| < |r_2| \tag{3}$$

и т. д. На каждом шаге новый остаток меньше остатка на предыдущем шаге,

$$|b| > |r_1| > |r_2| > \ldots,$$

и на каком-то k-м шаге ($k < |b|$) остаток станет равным нулю:

k-й шаг.

$$r_{k-2} = q_k \cdot r_{k-1}. \tag{k}$$

Покажем, что последний не равный нулю остаток r_{k-1} является искомым (a, b). Действительно, мы имеем цепочку равенств:

(1) $\quad a = q_1 \cdot b + r_1,$

(2) $\quad b = q_2 \cdot r_1 + r_2,$

(3) $\quad r_1 = q_3 \cdot r_2 + r_3,$

. . . . . .

$(k-1)$ $\quad r_{k-3} = q_{k-1} \cdot r_{k-2} + r_{k-1},$

(k) $\quad r_{k-2} = q_k \cdot r_{k-1}.$

Из последнего равенства имеем $r_{k-1} | r_{k-2}$, из предпоследнего — $r_{k-1} | r_{k-1}$ и $r_{k-1} | r_{k-2}$ и, следовательно, $r_{k-1} | r_{k-3}$. Из предшествующего равенства аналогично заключаем, что $r_{k-1} | r_{k-4}$ и, поднимаясь таким образом к все более и более

ранним равенствам, заключаем, что..., $r_{k-1} \mid r_2$, $r_{k-1} \mid r_1$, $r_{k-1} \mid b$, $r_{k-1} \mid a$. Мы видим, что r_{k-1} — общий делитель чисел a и b.

Пусть теперь $c \mid a$ и $c \mid b$. Тогда из (1), (2),..., $(k-1)$ последовательно получаем: $c \mid r_1$, $c \mid r_2$,..., $c \mid r_{k-1}$. Таким образом, r_{k-1} — действительно НОД чисел a и b.

Рассмотрим числовой пример: $a = 858$, $b = 253$. Имеем:

$$
\begin{aligned}
&(1) \quad 858 = 3 \cdot 253 + 99,\\
&(2) \quad 253 = 2 \cdot 99 + 55,\\
&(3) \quad 99 = 1 \cdot 55 + 44,\\
&(4) \quad 55 = 1 \cdot 44 + 11,\\
&(5) \quad 44 = 4 \cdot 11,
\end{aligned}
$$

откуда $(858, 253) = 11$. Итак, с помощью алгоритма Евклида НОД двух чисел находится без использования разложения этих чисел на простые сомножители.

В теореме 3 мы установили, что $(a, b) = d$ представимо в виде

$$d = s \cdot a + t \cdot b,$$

но в доказательстве не было никакого указания на то, как найти соответствующие числа s и t. С помощью алгоритма Евклида эта задача решается очень просто. Мы не будем описывать процедуру в общем случае, а поясним ее на уже разобранном числовом примере.

Итак, нужно найти такие целые числа s и t, что

$$11 = s \cdot 858 + t \cdot 253.$$

Из (4), (3), (2), (1) последовательно получаем:

$$
\begin{aligned}
11 &= 55 + (-1) \cdot 44,\\
44 &= 99 + (-1) \cdot 55,\\
55 &= 253 + (-2) \cdot 99,\\
99 &= 858 + (-3) \cdot 250.
\end{aligned}
$$

Подставляя теперь в первое из выписанных сейчас равенств выражение для 44 из второго, затем для 55 — выражение из следующего равенства и т. д., получаем:

$$
\begin{aligned}
11 &= 55 + (-1) \cdot (99 + (-1) \cdot 55) =\\
&= 2 \cdot 55 + (-1) \cdot 99 =\\
&= 2 \cdot (253 + (-2) \cdot 99) + (-1) \cdot 99 =\\
&= 2 \cdot 253 + (-5) \cdot 99 =\\
&= 2 \cdot 253 + (-5) \cdot (858 + (-3) \cdot 253) =\\
&= (-5) \cdot 858 + 17 \cdot 253.
\end{aligned}
$$

Окончательно: $s = -5$, $t = 17$.

Читатель легко уяснит себе, как применяется алгоритм в общем случае. Равенства, возникающие в алгоритме Евклида при нахождении НОД чисел a и b, позволяют решить в целых числах уравнение вида

$$d = xa + yb,$$

(где $d = (a, b)$).

Вообще, уравнение вида

$$xa + yb = c,$$

где a, b, c — заданные целые числа, для которого ищется целочисленное решение x, y, называется *линейным диофантовым уравнением* с двумя неизвестными. Линейным оно называется потому, что неизвестные x и y входят в него в первой степени. Термин «диофантово» [1]) указывает на то, что коэффициенты уравнения — целые числа и что решения также ищутся целочисленные.

Заметим, что мы в действительности уже научились решать линейные диофантовы уравнения вида

$$xa + yb = c. \qquad (I)$$

Но мы должны обсудить вопрос о всех решениях уравнения (I) более детально. Отметим сначала, что не всякое уравнение такого вида имеет решение. Действительно, если уравнение (I) имеет решение в целых числах, скажем, $x = x_0$, $y = y_0$: $c = x_0a + y_0b$, и если $d = (a, b)$, то, так как $d|a$, $d|b$, d делит оба слагаемых в правой части и, следовательно, также делит c. Отсюда заключаем, что

Для существования целочисленного решения уравнения (I) *необходимо, чтобы правая часть уравнения делилась на* НОД *чисел* a *и* b.

Например, уравнение

$$9x + 15y = 7$$

решения не имеет, так как 7 не делится на $3 = (9,15)$. Наоборот, если $d|c$, то уравнение (I) имеет целочисленное решение и мы даже знаем, как такое решение найти. Действительно, пусть $c = c'd$, и пусть s и t — такие целые числа (их

[1]) По имени древнегреческого математика Диофанта (около 250 г. до н. э.), который в своей книге «Арифметика» исследовал целочисленные уравнении. В конце нашего изложения мы немного остановимся на квадратичных диофантовых уравнениях.

можно найти с помощью алгоритма Евклида), что

$$d = as + bt.$$

Тогда

$$c = c'd = a(sc') + b(tc'),$$

т. е. $x_0 = sc'$, $y_0 = tc'$ — решение уравнения (I).

Решим, например, диофантово уравнение

$$33 = 858x + 253y. \qquad \text{(II)}$$

Выше мы показали, что

$$11 = 858 \cdot (-5) + 253 \cdot 17.$$

Умножая это равенство почленно на 3, получаем

$$33 = 858 \cdot (-15) + 253 \cdot 51.$$

Итак, $x = -15$, $y = 51$ — решение уравнения (II). Не следует думать, что найденное решение единственно. Вообще, оказывается, что *если диофантово уравнение вида* (I) *имеет решение, то оно имеет бесконечно много решений.* Мы сейчас исследуем этот вопрос более подробно: докажем сформулированное утверждение и найдем общий вид всевозможных решений уравнения (I). Начнем с выяснения общего вида. Предположим, что мы уже знаем, что наряду с целочисленным решением x_0, y_0 уравнение (I) имеет еще и решение x_1, y_1. Имеем:

$$c = ax_0 + by_0,$$

$$c = ax_1 + by_1.$$

Вычитая второе равенство из первого, получаем:

$$a(x_0 - x_1) + b(y_0 - y_1) = 0,$$

или

$$a(x_0 - x_1) = b(y_1 - y_0). \qquad \text{(III)}$$

Если $d = (a, b)$, то положим $a' = a/d$, $b' = b/d$, т. е.

$$a = a'd,$$

$$b = b'd,$$

где a' и b' — взаимно простые числа. Сокращая равенство (III) на d, приходим к равенству

$$a'(x_0 - x_1) = b'(y_1 - y_0),$$

Но тогда, так как a', b' взаимно просты, $a' | (y_1 - y_0)$ и, аналогично, $b' | (x_0 - x_1)$. Положив

$$y_1 - y_0 = a'k_1,$$
$$x_0 - x_1 = b'k_2,$$

имеем $a'b'k_1 = a'b'k_2$, откуда $k_1 = k_2 = k$. Таким образом, окончательно

$$y_1 = y_0 + a'k = y_0 + \frac{a}{d}k, \qquad \text{(IV)}$$

$$x_1 = x_0 - b'k = x_0 - \frac{b}{d}k, \qquad \text{(V)}$$

где k — некоторое целое число. Обратно, легко проверить, что если x_0, y_0 — решение уравнения (I), то все пары чисел (IV), (V) при произвольном целочисленном k дают решение уравнения (I). Действительно,

$$\begin{aligned} ax_1 + by_1 &= a\left(x_0 - \frac{b}{d}k\right) + b\left(y_0 + \frac{a}{d}k\right) = \\ &= ax_0 + by_0 + \left(-\frac{ab}{d}k + \frac{ab}{d}k\right) = \\ &= c + 0 = c. \end{aligned}$$

Итак, *если* x_0, y_0 — *решение уравнения* (I), *то все числа вида* $x_0 - \frac{b}{d}k$, $y_0 + \frac{a}{d}k$ *являются также решениями* (значит, решений, во всяком случае, бесконечно много — по одному для каждого k) *и других решений нет.*

§ 4. ГАУССОВЫ ЧИСЛА И ЦЕЛЫЕ ГАУССОВЫ ЧИСЛА

Естественным обобщением целых рациональных чисел являются «целые комплексные числа» или, как их обычно называют, «целые гауссовы числа» по имени великого немецкого математика К. Ф. Гаусса, который их впервые подробно изучал.

Определение 4. *Целым гауссовым числом* называется комплексное число, вещественная и мнимая части которого суть целые рациональные числа. Иначе говоря, это комплексные числа α вида

$$\alpha = a + bi, \qquad \text{(1)}$$

где a и b — целые (рациональные) числа. Наряду с целыми гауссовыми числами нам понадобятся также (просто) *гауссовы числа*, т. е. комплексные числа, у которых вещественная и мнимая части — числа рациональные.

Связь между областями гауссовых чисел и целых гауссовых чисел аналогична связи между рациональными числами и целыми рациональными числами. Более точно, имеются в виду следующие утверждения, которыми в дальнейшем мы будем часто пользоваться без особой оговорки и которые читатель легко проверит непосредственно:

I. *Сумма, разность и произведение двух целых гауссовых чисел также являются целыми гауссовыми числами* (это свойство выражают кратко, говоря, что целые гауссовы числа образуют к о л ь ц о).

II. *Сумма, разность, произведение и частное* (в случае если делитель не равен нулю) *двух гауссовых чисел также являются гауссовыми числами* (это свойство выражают кратко словами: гауссовы числа образуют п о л е).

III. *Частное двух целых гауссовых чисел является гауссовым числом и, обратно, всякое гауссово число представимо как частное двух целых гауссовых чисел.*

Небольшого пояснения требует последнее утверждение. Пусть $\alpha = a + bi$ и $\beta = c + di$ — целые гауссовы числа (т. е. a, b, c, d — целые рациональные числа) и пусть $\beta \neq 0$. Покажем, что $\gamma = \alpha/\beta$ — гауссово число. Действительно,

$$\gamma = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + dd - adi + bci}{c^2 + d^2} =$$

$$= \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i.$$

Числа $\frac{ac + bd}{c^2 + d^2}$ и $\frac{bc - ad}{c^2 + d^2}$ — вещественная и мнимая части числа γ — числа рациональные и, следовательно, γ — гауссово число.

Отметим, наконец, что, очевидно, всякое рациональное число является гауссовым (мнимая часть равна 0) и что всякое целое рациональное число является целым гауссовым числом.

Для дальнейшего полезно представить себе расположение целых гауссовых чисел на комплексной плоскости. По самому своему определению целые гауссовы числа представляются точками с целочисленными координатами (рис. 1).

Они лежат в вершинах сетки квадратов со стороной, равной 1, покрывающей комплексную плоскость.

Из теории комплексных чисел нам понадобятся понятия нормы и модуля комплексного числа. Напомним, что *нормой* комплексного числа $\alpha = x + iy$ называется неотрицательное вещественное число $N(\alpha) = x^2 + y^2$; *модулем* комплексного числа α, обозначаемым $|\alpha|$, называется вещественное число $\sqrt{x^2 + y^2}$. Геометрически модуль комплексного

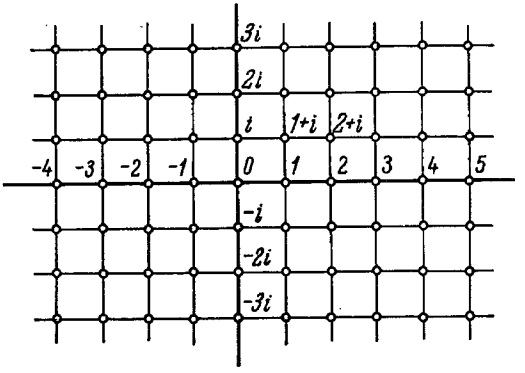

Рис. 1.

числа — это расстояние соответствующей точки на комплексной плоскости от начала координат. Норма $N(\alpha)$ числа α представима как произведение $N(\alpha) = \alpha \cdot \bar{\alpha}$, где $\bar{\alpha}$ — комплексно сопряженное число $x - iy$ числа α. Известным предполагается также свойство мультипликативности нормы, т. е. что

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta). \qquad (2)$$

Отметим сразу, что если α — гауссово число, то $N(\alpha)$ — неотрицательное рациональное число, а если α — даже целое гауссово число, то $N(\alpha)$ — неотрицательное целое число [1]).

Однако не всякое положительное целое рациональное число является нормой целого гауссового числа. Действительно, мы докажем сейчас следующую теорему:

---

[1]) Модуль $|\alpha|$ гауссова числа уже не обязан быть рациональным числом, поэтому в дальнейшем мы в основном будем пользоваться не модулем, а нормой.

Теорема 7. *Положительное целое рациональное число c является нормой некоторого целого гауссова числа тогда и только тогда, когда число c представимо в виде суммы двух квадратов целых чисел.*

Доказательство. Если $\alpha = a + bi$ — целое гауссово число, то $N(\alpha) = a^2 + b^2$ — сумма квадратов целых чисел a и b. Наоборот, если $c = x^2 + y^2$, где x и y — целые рациональные числа, то $c = N(x + yi)$, где $x + yi$ — целое гауссово число. Теорема доказана.

Нетрудно показать, что не всякое положительное целое число представимо в виде суммы двух квадратов. Покажем, например, что нечетное положительное целое число t, представимое в виде суммы двух квадратов целых чисел, дает при делении на четыре остаток, равный 1, т. е. является числом вида $t = 4k + 1$. Действительно, пусть $t = x^2 + y^2$, тогда одно из чисел, скажем, x, должно быть четным, другое — y — нечетным. Пусть $x = 2m$ и $y = 2n + 1$. Тогда $x^2 = 4m^2$ и $y^2 = 4(n^2 + n) + 1$ и, окончательно, $t = 4(m^2 + n^2 + n) + 1$, что и доказывает наше утверждение. Таким образом, числа 7, 11, 15 и др. непредставимы в виде суммы двух квадратов и не являются, следовательно, нормами гауссовых чисел.

Вопрос о том, какие в точности целые числа представимы в виде суммы двух квадратов или, что то же самое, какие числа являются нормами целых гауссовых чисел, мы выясним в результате исследования арифметики целых гауссовых чисел. К исследованию этой арифметики мы теперь и переходим.

Как и в области (кольце) целых рациональных чисел, так и в области целых гауссовых чисел основной интерес представляет вопрос делимости.

Мы будем говорить, что целое гауссово число α делит целое гауссово число β — и записывать этот факт через $\alpha \mid \beta$—если для некоторого целого гауссова числа γ имеет место равенство

$$\beta = \alpha \cdot \gamma. \tag{3}$$

Так как из (3) следует $N(\beta) = N(\alpha) \cdot N(\gamma)$, то необходимым условием для $\alpha \mid \beta$ является делимость $N(\alpha) \mid N(\beta)$, где $N(\alpha)$ и $N(\beta)$ — целые рациональные числа.

В случае целых рациональных чисел имеются только два числа, которые делят все целые числа: $+1$ и -1: в случае целых гауссовых чисел таких чисел имеется четыре:

$+1$, -1, $+i$, $-i$. Сразу видно, что указанные четыре числа этим свойством обладают. Действительно,

$$\alpha = \alpha \cdot 1,$$
$$\alpha = (-\alpha) \cdot (-1),$$
$$\alpha = (-\alpha i) \cdot i,$$
$$\alpha = (\alpha i) \cdot (-i).$$

Других чисел с данными свойствами среди целых гауссовых чисел нет. Действительно, если некоторое целое гауссово число ξ делит все целые гауссовы числа, то оно, в частности, должно делить число 1 (поэтому такие числа называются *делителями единицы*). Из $N(\xi) \mid 1$ следует, что $N(\xi) = 1$. Если $\xi = x + yi$, то $x^2 + y^2 = 1$. Очевидно, что это уравнение имеет в целых рациональных числах в точности четыре решения: $x = 1$, $y = 0$; $x = -1$, $y = 0$; $x = 0$, $y = 1$; $x = 0$, $y = -1$. Эти четыре решения как раз и соответствуют целым гауссовым числам $+1$, -1, i, $-i$.

Для целых гауссовых чисел, аналогично тому, как это делалось для целых рациональных чисел, определяются понятия *общего делителя*, *наибольшего общего делителя*, *взаимно простых чисел* и *простых чисел*. Первые три понятия дословно определяются как и в случае целых рациональных чисел. Однако на определении простого целого гауссова числа нужно остановиться несколько более подробно.

Определение 5. Целое гауссово число π называется *простым*, если в любом его разложении $\pi = \tau \cdot \sigma$ в произведение двух целых гауссовых чисел один из сомножителей (τ или σ) является делителем единицы (при этом делители единицы простыми числами не считаются).

Иначе это свойство можно выразить так: простое гауссово число π — это такое целое гауссово число, отличное от нуля, норма которого больше единицы и которое не разложимо в произведение двух целых гауссовых чисел, нормы которых меньше, чем норма числа π.

Согласно этому определению простыми гауссовыми числами будут, например, числа $\pi_1 = 2 + i$ ($N(\pi_1) = 5$), $\pi_2 = 3 + 2i$ ($N(\pi_2) = 13$). Вообще, простыми числами будут все числа, нормы которых являются простыми рациональными числами. В дальнейшем мы увидим, что этими примерами простые гауссовы числа не исчерпываются. В ходе наших исследований мы опишем все простые гауссовы числа.

Теперь же перейдем к формулировке и к доказательству основной теоремы арифметики целых гауссовых чисел.

Основная теорема. *Всякое целое гауссово число* $\alpha \neq 0$ *разложимо в произведение простых гауссовых чисел*

$$\alpha = \pi_1 \cdot \pi_2 \ldots \pi_k \tag{4}$$

(π_l — простые гауссовы числа, не обязательно все различные). *Такое разложение однозначно в следующем смысле: если*

$$\alpha = \sigma_1 \cdot \sigma_2 \ldots \sigma_l \tag{5}$$

— другое разложение числа α *в произведение простых гауссовых чисел* σ_j, *то оба разложения обладают одним и тем же числом сомножителей,* $k = l$, *и разложения* (4) *и* (5) *могут отличаться друг от друга только порядком следования сомножителей и множителями, являющимися делителями единицы.*

Относительно части формулировки, касающейся однозначности разложения, сделаем еще одно замечание. Если, скажем,

$$\alpha = \pi_1 \cdot \pi_2 \cdot \pi_3$$

— произведение простых чисел π_1, π_2, π_3, то, например,

$$\alpha = (-\pi_3) \cdot (i\pi_2) \cdot (i\pi_1) \qquad (= \pi_1 \cdot \pi_2 \cdot \pi_3)$$

— «другое» представление числа α в виде произведения простых чисел—π_3, $i\pi_2$, $i\pi_1$, отличных от простых чисел π_1, π_2, π_3. Однако легко заметить, что любое из чисел $-\pi_3$, $i\pi_2$, $i\pi_1$ получается умножением какого-то из чисел π_1, π_2, π_3 на некоторый делитель единицы; при этом изменен также первоначальный порядок чисел. Такие различия в разложениях одного и того же числа допускаются. Вторая часть формулировки теоремы как раз и утверждает, что подобного рода различными разложениями неоднозначность представления исчерпывается. Это обстоятельство ничем не отличается от ситуации в арифметике целых рациональных чисел. Оно лишь усложняется тем, что в случае арифметики целых гауссовых чисел мы располагаем бо́льшим числом делителей единицы [1]). Утверждение об однозначности

[1]) Отметим, что однозначность разложения с точностью до знаков сомножителей, о которой шла речь в случае целых рациональных чисел, и означает как раз однозначность с точностью до множителей, являющихся делителями единицы, так как $+1$ и -1—единственные делители единицы в этом случае.

разложения можно сформулировать короче, если ввести понятие ассоциированности целых гауссовых чисел.

Определение 6. Два целых гауссовых числа называются *ассоциированными*, если они отличаются друг от друга на сомножитель, равный делителю единицы, т. е. β, $-\beta$, $i\beta$, $-i\beta$ — ассоциированные целые гауссовы числа, если β — произвольное целое гауссово число.

С использованием этого определения утверждение об однозначности в основной теореме формулируется так:

Если $\alpha = \pi_1 \cdot \pi_2 \ldots \pi_k$ *и* $\alpha = \sigma_1 \cdot \sigma_2 \ldots \sigma_l$, *где* π_i $(i = 1, 2, \ldots, k)$ *и* σ_j $(j = 1, 2, \ldots, l)$ — *простые числа, то* $l = k$ *и сомножители* σ_j *можно так переставить, что каждое* σ_j *будет ассоциировано с соответствующим простым числом* π_j.

Наметим доказательство основной теоремы. Оно проводится почти дословно так же, как и доказательство соответствующих утверждений для целых рациональных чисел. Именно поэтому мы его подробно приводить и не будем, но очень рекомендуем читателю проделать это самостоятельно.

Первое утверждение теоремы — о существовании разложения — можно провести индукцией по норме числа:

а) Если $N(\alpha) = 1$, то $\alpha = 1, -1, i, -i$, т. е. число α разложимо в произведение пустого множества простых чисел [1]).

б) Пусть $N(\alpha) = n$, а для всех целых гауссовых чисел с меньшей нормой утверждение уже доказано. Тогда или α — простое число и все доказано, или $\alpha = \rho \cdot \tau$, где $N(\rho) < n$ и $N(\tau) < n$. По предположению индукции, для ρ и τ разложения существуют: $\rho = \pi_1 \cdot \pi_2 \ldots \pi_k$ и $\tau = \sigma_1 \cdot \sigma_2 \ldots \sigma_l$, тогда $\alpha = \pi_1 \cdot \pi_2 \ldots \pi_k \cdot \sigma_1 \cdot \sigma_2 \ldots \sigma_l$ — разложение для α.

Доказательство утверждения об однозначности можно вести по пути установления свойств наибольшего общего делителя и свойств взаимно простых чисел в области целых гауссовых чисел. Ключом для всего доказательства является утверждение о возможности деления с остатком в области целых гауссовых чисел. Оно формулируется здесь так:

Пусть α, β $(\beta \neq 0)$ — *два целых гауссовых числа, тогда существуют такие целые гауссовы числа* γ *и* ρ, *причем* $N(\rho) < N(\beta)$, *что*

$$\alpha = \gamma \cdot \beta + \rho.$$

---

[1]) Относительно «разложимости» делителей единицы в произведение простых сомножителей мы принимаем то же соглашение, что и для ± 1 в случае целых рациональных чисел; см. стр. 7.

Доказательство основано на очень простом геометрическом факте: если P — точка, лежащая внутри квадрата со стороной a, или на одной из его сторон, то расстояние от точки P до ближайшей вершины меньше, чем a. Действительно, точка, наиболее удаленная от всех вершин,— это

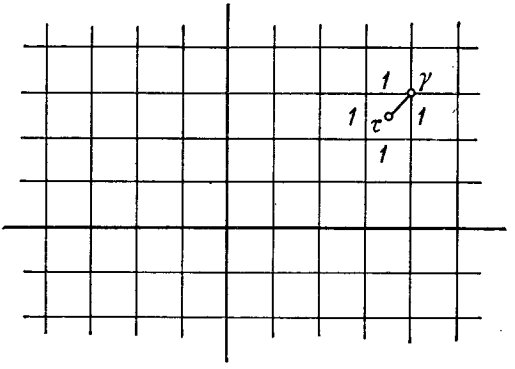

Рис. 2.

центр квадрата. Но расстояние от нее до любой вершины равно $\frac{1}{\sqrt{2}}a < a$. Любая другая точка квадрата отдалена от ближайшей вершины еще меньше.

Из этого простого утверждения теперь сразу же видно, что для любой точки τ комплексной плоскости найдется точка γ с целыми координатами — точка, представляющая целое гауссово число,— отдаленная от τ меньше, чем на 1 (рис. 2). Иначе говоря, для всякого комплексного числа τ существует такое целое гауссово число γ, что $N(\tau - \gamma) < 1$. Найдем такое γ для числа $\tau = \alpha/\beta$ и положим $\rho = \alpha - \gamma\beta$. Тогда ρ — целое гауссово число,

$$N(\rho) = N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta)$$

и

$$\alpha = \gamma\beta + \rho.$$

Утверждение доказано.

Имея уже теорему о делении с остатком, все остальные свойства можно доказать так же, как мы это делали выше в случае рациональных чисел: 1) доказывается существование НОД двух целых гауссовых чисел α, β как числа $\delta \neq 0$

с наименьшей нормой из множества чисел, представимых в виде $\alpha\xi + \beta\eta$ (ξ и η — целые гауссовы числа), 2) вводится понятие взаимно простых гауссовых целых чисел и доказывается основная лемма: если α взаимно просто с β_1 и α взаимно просто с β_2, то α взаимно просто с $\beta_1 \cdot \beta_2$. Затем уже совсем просто индукцией по норме доказывается однозначность разложения на простые сомножители.

§ 5. ПРОСТЫЕ ГАУССОВЫ ЧИСЛА И ПРЕДСТАВЛЕНИЕ ЦЕЛЫХ РАЦИОНАЛЬНЫХ ЧИСЕЛ В ВИДЕ СУММЫ ДВУХ КВАДРАТОВ

Перейдем теперь к описанию всех простых гауссовых чисел. Докажем сначала несколько вспомогательных утверждений — лемм.

Лемма 1. *Всякое простое гауссово число является делителем простого рационального числа* [1]).

Действительно, так как $N(\alpha) = \alpha \cdot \bar{\alpha}$, *то всякое целое гауссово число делит свою норму*: $\alpha \mid N(\alpha)$. Пусть теперь π — простое гауссово число, тогда $\pi \mid N(\pi)$, и пусть $N(\pi) = p_1 \cdot p_2 \ldots p_r$ — разложение числа $N(\pi)$ в произведение простых рациональных чисел. Имеем: $\pi \mid p_1 \cdot p_2 \ldots p_r$, следовательно, π делит одно из простых чисел p_i. Действительно, если бы простое целое гауссово число π не делило бы ни одно из чисел p_i, то оно было бы взаимно просто с каждым из них, а следовательно, и с их произведением $N(\pi)$. Но это невозможно, так как $\pi \mid N(\pi)$. Итак, число π является делителем одного из простых целых рациональных чисел p_i, — и лемма доказана.

Лемма 2. *Норма $N(\pi)$ простого гауссова числа π является или простым рациональным числом или квадратом простого рационального числа.*

Действительно, как мы уже знаем, π делит некоторое простое рациональное число p: пусть $p = \pi \cdot \gamma$. Перейдем

---

[1]) Заметим, что простое рациональное число является всегда и целым гауссовым числом, но как гауссово число оно не обязательно простое, а может делиться на целые гауссовы числа с меньшей нормой. Так, например, число 2 — простое, если его рассматривать как целое рациональное число, но оно не простое, если его рассматривать как целое гауссово число. Действительно, в области целых гауссовых чисел число 2 допускает разложение $2 = (1 + i) \cdot (1 - i)$ и ни один из сомножителей $1 + i$ и $1 - i$ не является делителем единицы. Очевидно, что и 5 не является простым в области гауссовых чисел, так как $5 = (2 + i)(2 - i)$.

к нормам: $N(\pi) \cdot N(\gamma) = p^2$. Возможны только два случая: 1) $N(\pi) = N(\gamma) = p$ и 2) $N(\pi) = p^2 = N(p)$, а $N(\gamma) = 1$. Лемма доказана.

Случай 2) означает, что γ — делитель единицы и что справедливо одно из равенств: $\pi = p$, $\pi = -p$, $\pi = ip$, $\pi = -ip$. Следовательно, p — такое простое рациональное число, которое одновременно является и простым гауссовым числом. В случае 1) γ — простое гауссово число, так как $N(\gamma) = p$. Можно утверждать, что $\gamma = \bar{\pi}$. Действительно, $N(\pi) = p = \pi \cdot \bar{\pi}$ и $\bar{\pi}$ — простое число. Но мы имеем также $p = \pi \cdot \gamma$, так что $\bar{\pi} = \gamma$.

С другой стороны, пусть p — какое-либо простое рациональное число, тогда, если оно не является простым гауссовым числом, то оно делится на какое-либо простое гауссово число, отличное от p, и при этом, как мы видели, $p = \pi \cdot \bar{\pi}$, т. е. p является произведением двух простых гауссовых комплексно сопряженных чисел. В этом случае p является нормой целого гауссового числа и, следовательно, представимо в виде суммы двух квадратов. Такое простое число, если оно нечетное (т. е. $p \neq 2$),— число вида $4n + 1$. Можно показать, что *все простые числа вида* $4n + 1$ *представимы в виде суммы двух квадратов*, т. е. являются нормами некоторых целых гауссовых чисел, а потому не являются простыми гауссовыми числами и, следовательно, принадлежат к классу тех простых рациональных чисел, которые разложимы в произведение двух комплексно сопряженных простых гауссовых чисел. Доказательство этого утверждения мы приводить не будем [1]). Все простые рациональные числа, отличные от чисел вида $4n + 1$ и от числа 2, т. е. числа вида $4n + 3$, и составляют как раз множество простых рациональных чисел, остающихся простыми и в области гауссовых чисел.

Несколько особое положение занимает простое число 2. Легко видеть, что

$$2 = i \cdot (1 - i)^2,$$

$N(1 - i) = 2$. Таким образом, 2 делится на квадрат простого гауссова числа $(1 - i)$.

---

[1]) Доказательство этого факта, основанное на теории сравнений и восходящее к Л. Эйлеру, можно найти почти во всех учебниках по теории чисел. Особенно подробно оно изложено в книге [3] из приведенного в конце брошюры списка литературы.

Предполагая известным, что все простые числа вида $4n + 1$ представимы в виде суммы двух квадратов, мы можем теперь установить, каковы все целые рациональные числа, представимые в виде суммы двух квадратов. Как мы уже знаем, для всякого числа t с таким свойством необходимо и достаточно, чтобы оно было нормой некоторого целого гауссового числа α: $t = N(\alpha)$. Число α разлагается в произведение простых гауссовых чисел:

$$\alpha = \pi_1 \cdot \pi_2 \ldots \pi_r. \tag{6}$$

Разобьем все простые числа π_i ($i = 1, 2, \ldots, r$) на два класса: в первый класс соберем те числа π_i, нормы которых — простые числа, а во второй, соответственно, числа, нормы которых — квадраты простых чисел [1]). Обозначим различные числа первого класса через σ_j ($j = 1, 2, \ldots, l$), а все различные числа второго класса — через ρ_k ($k = 1, 2, \ldots, s$). Имеем: $N(\sigma_j) = p_j$, $N(\rho_k) = q_k^2$, где p_j — простое число вида $4n + 1$ или 2, а q_k — простое число вида $4n + 3$. Объединяя равные простые числа в правой части (6), запишем это произведение в виде степеней простых чисел σ_j и ρ_k:

$$\alpha = \sigma_1^{a_1} \ldots \sigma_l^{a_l} \cdot \rho_1^{b_1} \ldots \rho_s^{b_s}, \tag{7}$$

и, переходя к нормам, имеем

$$N(\alpha) = t = N(\sigma_1^{a_1}) \ldots N(\sigma_l^{a_l}) \cdot N(\rho_1^{b_1}) \ldots N(\rho_s^{b_s}),$$

$$t = p_1^{a_1} \ldots p_l^{a_l} q_1^{2b_1} \ldots q_s^{2b_s}. \tag{8}$$

Мы видим, что простые числа q_k входят в разложение числа t в четных степенях. Обратно, пусть число t представимо в виде (8), где каждое p_j — простое число вида $4n + 1$ или число 2, q_k — простые числа вида $4n + 3$ и $a_1, \ldots, a_l, b_1, \ldots, b_s$ — целые неотрицательные числа. Тогда, поскольку каждое p_j является суммой двух квадратов, можно подобрать σ_j так, чтобы $N(\sigma_j) = p_j$. Положив, далее, $\rho_k = q_k$ и, наконец, $\alpha = \sigma_1^{a_1} \ldots \sigma_l^{a_l} \cdot \rho_1^{b_1} \ldots \rho_s^{b_s}$, получим $t = N(\alpha)$, т. е. t представимо в виде суммы двух квадратов. Окончательно имеем следующую теорему:

Теорема 8. *Для того чтобы целое рациональное число было представимо в виде суммы двух квадратов,*

---

[1]) Может, конечно, оказаться, что один из классов пуст. Это, однако, не повлияет существенно на ход наших рассуждений: надо будет только иметь в виду, что все числа a_j или все числа b_k (в разложениях (7) и (8)) могут быть нулями.

необходимо и достаточно, чтобы простые числа вида $4n+3$ *входили в разложение этого числа на простые сомножители в четных степенях* [1]).

Как мы видим, эта теорема дает критерий того, чтобы диофантово уравнение второй степени вида

$$x^2 + y^2 = t$$

имело решение (целочисленное). На том, как такое решение фактически находится, мы здесь останавливаться не будем.

Вообще же, изучение диофантовых уравнений вида

$$ax^2 + 2bxy + cy^2 = t$$

тесно связано с арифметиками в областях чисел, аналогичных области целых гауссовых чисел.

Существенным в таких исследованиях оказывается следующий удивительный факт, с которым столкнулись математики в середине прошлого столетия: *не во всех подобных арифметиках имеет место теорема об однозначном разложении чисел в произведение простых чисел.* Не входя в детали возникшей здесь ситуации, мы приведем пример «арифметики», где основная теорема не выполняется.

§ 6. ЕЩЕ ОДНА «АРИФМЕТИКА»

Будем рассматривать комплексные числа вида

$$\alpha = x + y\sqrt{-5}, \qquad (1)$$

где x и y — целые рациональные числа. Легко видеть, что сумма, разность и произведение чисел вида (1) опять являются числами такого же вида. Обозначим совокупность всех чисел вида (1) через Γ. Очевидно, что Γ содержит все целые рациональные числа (при $y=0$). Так же как в случаях целых рациональных и целых гауссовых чисел, можно говорить о делимости в Γ: α делит β ($\alpha \mid \beta$), если β/α — опять число из Γ, т. е. представимо в виде (1). Как и в случае целых гауссовых чисел, в вопросе делимости важную роль играют нормы чисел из Γ:

$$N(\alpha) = N(x + y\sqrt{-5}) =$$
$$= (x + y\sqrt{-5})(x - y\sqrt{-5}) = x^2 + 5y^2.$$

Таким образом, норма всякого числа из Γ есть целое рациональное число и, так как $N(\xi \cdot \eta) = N(\xi) \cdot N(\eta)$, то необходимым (но вообще говоря, не достаточным) условием для $\alpha \mid \delta$ является условие $N(\alpha) \mid N(\beta)$.

[1]) Такая формулировка охватывает и случай, когда простых чисел вида $4n+3$ нет в разложении рассматриваемого числа, — ведь число 0 также является четным!

Так же как и в случае целых гауссовых чисел, естественно вводится понятие делителей единицы и простых чисел. В отношении делителей единицы дело обстоит здесь даже проще, чем для целых гауссовых чисел. А именно, делителями единицы являются только числа ± 1. Действительно, для делителей единицы $\xi = u + v\sqrt{-5}$ должно выполняться условие $N(\xi) = u^2 + 5v^2 = 1$. Но это диофантово уравнение, очевидно, не может иметь решений, отличных от $u = \pm 1$ и $v = 0$.

Тот факт, что каждое число нз Г представимо в виде произведения простых чисел из Г, доказывается индукцией по норме дословно так же, как и в случае целых гауссовых чисел. А вот утверждение об однозначности такого разложения здесь уже не верно, и мы это покажем на простом примере.

Покажем сначала, что числа $2 = 2 + 0\cdot\sqrt{-5}$, $3 = 3 + 0\cdot\sqrt{-5}$, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ — простые числа в Г. Действительно, $N(2) = 4$, $N(3) = 9$, $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. Если бы одно из этих чисел не было простым в Г, то оно могло бы делиться только на некоторое число $\alpha = x + y\sqrt{-5}$, для которого $N(\alpha) = x^2 + 5y^2 = 2$ или $N(\alpha) = x^2 + 5y^2 = 3$. Но таких чисел в Г нет, так как очевидно, что уравнения

$$x^2 + 5y^2 = 2 \tag{2}$$

и

$$x^2 + 5y^2 = 3 \tag{3}$$

не имеют целочисленных решений.

Итак, указанные четыре числа — простые числа в Г. Отметим теперь легко проверяемое равенство

$$6 = 2\cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{4}$$

Оно показывает, что чнсло 6 из Г имеет два различнык представления в виде пронзведения простых чисел.

С отмеченным явлением столкнулся немецкий математик Э. Куммер (1810—1893) при своих попытках решить так называемую великую теорему Ферма. В дальнейшем трудности, возникающие в связи с невыполнением основной теоремы арифметикн в некоторых важных областях чисел, были успешно преодолены как самим Куммером, так и другими математиками — Р. Дедекиндом, Е. Золотаревым, Л. Кронекером и др. Возникла большая новая область в математике — теория алгебраических чисел, которая успешно развивается вплоть до наших дней.

ЛИТЕРАТУРА

Мы укажем ряд изданий, в которых читатель может найти дополнительные сведения по теории чисел и, в частности, по теме нашего изложения. Предлагаемый список не претендует на полноту. Некоторые из указанных работ в свою очередь содержат указание на литературу по теории чисел. Мы рассмотрим книги по возрастающей трудности. Если первые из указанных работ не требуют подготовки, выходящей за рамки школьной математики, то последние представляют собой учебники для студентов университетов и пединститутов. Как показывает опыт, ими можно также пользоваться для самообразования.

1. А. Я. Хинчин, Элементы теории чисел, Энциклопедия элементарной математики, кн. I, Арифметика, Гостехиздат, 1951.

Эта статья крупного советского математика А. Я. Хинчина написана с большим мастерством и может быть рекомендована как учителям, так и школьникам старших классов. Глава I «Делимость и простые числа» содержит, в частности, подробное доказательство основной теоремы арифметики. Глава II «Метод сравнений» является, на наш взгляд, одним из лучших введений в теорию сравнений — раздел теории чисел, имеющий очень большое число приложений как в арифметике, так и в современной алгебре.

2. А. И. Маркушевич, Деление с остатком в арифметике и в алгебре (сер. «Педагогическая библиотека учителя»), изд. Академии педагогических наук РСФСР, 1949.

Книга содержит почти весь материал, излагаемый в нашей брошюре, но, кроме того, и ряд других разделов алгебры и арифметики, непосредственно примыкающих к теории делимости.

3. Г. Дэвенпорт, Высшая арифметика, «Наука», 1965.

Подзаголовок книги «Введение в теорию чисел» уже указывает на то, что в ней дается систематическое изложение начал этой области. Написана она крупным английским специалистом по теории чисел. Книга Дэвенпорта не предполагает познаний, выходящих за пределы школьной математики. Она особенно может быть рекомендована студентам-математикам младших курсов, но доступна и не математикам. От последних, правда, потребуются некоторые навыки для хорошего понимания изложения. Для читателей нашей брошюры, несомненно, интересной будут глава II «Сравнения», а также глава V «Суммы квадратов», в которой дается полное доказательство представимости простых чисел вида $4n + 3$ в виде суммы двух квадратов.

В качестве собственно учебников по теории чисел, предназначенных для студентов-математиков, можно порекомендовать:

4. И. Н. Виноградов, Основы теории чисел, «Наука», 1965.
5. И. В. Арнольд, Теоретическая арифметика, Учпедгиз, 1939.
6. А. А. Бухштаб, Теория чисел, «Просвещение», 1966.
7. Г. Хассе, Лекции по теории чисел, ИЛ, 1953.

Цена 5 коп.

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ

Вып. 1. А. И. Маркушевич. Возвратные последовательности.
Вып. 2. И. П. Натансон. Простейшие задачи на максимум и минимум
Вып. 3. И. С. Соминский. Метод математической индукции.
Вып. 4. А. И. Маркушевич. Замечательные кривые.
Вып. 5. П. П. Коровкин. Неравенства.
Вып. 6. Н. Н. Воробьев. Число Фибоначчи.
Вып. 7. А. Г. Курош. Алгебраические уравнения произвольных степеней.
Вып. 8. А. О. Гельфонд. Решение уравнений в целых числах.
Вып. 9. А. И. Маркушевич. Площади и логарифмы.
Вып 10. А. С. Смогоржевский. Метод координат.
Вып. 11. Я. С. Дубнов. Ошибки в геометрических доказательствах.
Вып. 12. И. П. Натансон. Суммирование бесконечно малых величин.
Вып. 13. А. И. Маркушевич. Комплексные числа и конформные отображения.
Вып. 14. А. И. Фетисов. О доказательствах в геометрии.
Вып. 15. И. Р. Шафаревич. О решении уравнений высших степеней.
Вып. 16. В. Г. Шерватов. Гиперболические функции.
Вып. 17. В. Г. Болтянский. Что такое дифференцирование?
Вып. 18. Г. М. Миракьян. Прямой круговой цилиндр.
Вып. 19. Л. А. Люстерник. Кратчайшие линии.
Вып. 20. А. М. Лопшиц. Вычисление площадей ориентированных фигур.
Вып. 21. Л. И. Головина и И. М. Яглом. Индукция в геометрии.
Вып. 22. В. Г. Болтянский. Равновеликие и равносоставленные фигуры.
Вып. 23. А. С. Смогоржевский. О геометрии Лобачевского.
Вып. 24. Б. И. Аргунов и Л. А. Скорняков. Конфигурационные теоремы.
Вып. 25. А. С. Смогоржевский. Линейка в геометрических построениях.
Вып. 26. Б. А. Трахтенброт. Алгоритмы и машинное решение задач.
Вып. 27. В. А. Успенский. Некоторые приложения механики к математике.
Вып. 28. Н. А. Архангельский и Б. И. Зайцев. Автоматические цифровые машины.
Вып. 29. А. Н. Костовский. Геометрические построения одним циркулем.
Вып. 30. Г. Е. Шилов. Как строить графики.
Вып. 31. А. Г. Дорфман. Оптика конических сечений.
Вып. 32. Е. С. Вентцель. Элементы теории игр.
Вып. 33. А. С. Барсов. Что такое линейное программирование.
Вып. 34. Б. Е. Маргулис. Системы линейных уравнений.
Вып. 35. Н. Я. Виленкин. Метод последовательных приближений.
Вып. 36. В. Г. Болтянский. Огибающая.
Вып. 37. Г. Е. Шилов. Простая гамма (устройство музыкальной шкалы).
Вып. 38. Ю. А. Шрейдер. Что такое расстояние?
Вып. 39. Н. Н. Воробьев. Признаки делимости.
Вып. 40. С. В. Фомин. Системы счисления.
Вып. 41. Б. Ю. Коган. Приложение механики к геометрии.
Вып. 42. Ю. И. Любич и Л. А. Шор. Кинематический метод в геометрических задачах.
Вып. 43. В. А. Успенский. Треугольник Паскаля.
Вып. 44. И. Я. Бакельман. Инверсия.
Вып. 45. И. М. Яглом. Необыкновенная алгебра.
Вып. 46. И. М. Соболь. Метод Монте-Карло.
Вып. 47. Л. А. Калужнин. Основная теорема арифметики.